Solución NetLAN

Configuración del Acceso Remoto Internet

V 1.5 Junio de 2012

Índice

1. INTRODUCCIÓN

Esta guía describe los pasos que deben seguirse para que un usuario pueda conectarse a través de Internet a la RPV-IP de su empresa, mediante el software cliente IPSec.

El documento está divido en dos partes:

1. Una parte dirigida al administrador de la RPV-IP, en la que se describen los procesos de alta de usuario remoto y descarga del software IPSec con su correspondiente fichero de configuración.
2. Una segunda parte dirigida al usuario que quiere acceder a la RPV-IP, en la que se describe el proceso de instalación y el de configuración del software IPSec.

La presente guía es válida para la configuración de la Versión 4.6 (compatible con Windows 98, Windows Me y Windows NT), de la versión 5.0 (compatible con Windows Vista, Windows XP, Windows 2003 Server y Windows 2000) y de la versión 5.0.07.0290 (compatible con Windows7).

2. CONFIGURACIÓN DEL ACCESO IPSEC POR PARTE DEL ADMINISTRADOR DE LA RPV-IP

2.1 Gestión de Usuarios

Los usuarios que se vayan a conectar a la RPV-IP, deben estar dados de alta previamente; esta acción la realiza el Administrador siguiendo los pasos que se describen a continuación:

1) El administrador accederá a l Canal Online a través de la URL: http://www.movistar.es/netlan . En la pantalla que nos aparece pulsaremos el enlace '"Gestione su servicio Net-LAN" donde el sistema nos pedirá que nos autentiquemos con nuestro usuario de movistar



Figura 1: Acceso al Portal de Gestión

2) Tras autenticarse y seleccionar la pestaña '*Administración de su RPV-IP*', se selecciona la RPV-IP a gestionar (caso de que tenga varias), y accedemos al menú de administración



Figura 2: Selección de RPV-IP

3) Pulsando en el enlace '*aceptar*':



Figura 3: Gestión de usuarios de Remotos

Nos aparecen las distintas acciones que podemos realizar. El administrador tiene la posibilidad de:

- Búsqueda de usuarios (necesario para darlos de baja)
- Dar de alta usuarios
- Desactivación (temporal) de usuarios

Para RPV-IP's con varios usuarios existen opciones para:

- Dar de alta/baja usuarios a partir de una lista
- Dar de alta usuarios en bucle

Todas estas acciones se encuentran descritas con más detalle en la Guía del Administrador.

En nuestro caso daremos de alta un nuevo usuario seleccionando la *opción 'Alta de usuarios'*



Figura 4: Alta de nuevo usuario

Asignaremos un nombre y contraseña y pulsaremos '*aceptar*', de esta manera ya dispondremos de usuario para acceder a la RPV-IP.

2.2 Gestión de Cliente IPSec (Descarga del software)

Una vez que disponemos del usuario para acceder a la RPV-IP, es necesario descargar el software cliente IPSec y su correspondiente configuración. El software cliente IPSec lo encontraremos en el apartado ¿Necesita ayuda? Y dentro de la nueva pantalla que nos aparecen en la opción '*Configuración IPSec*'.

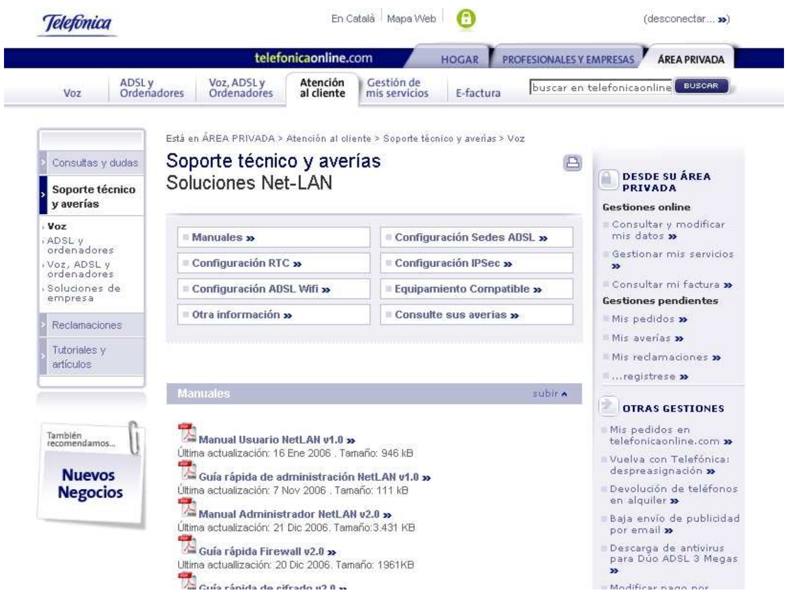


Figura 5: Descarga del software IPSec

Una vez descargado el software cliente IPSec que corresponda a nuestro sistema operativo, es necesario descargar la configuración del mismo. En el Portal de Gestión debemos seleccionar la pestaña correspondiente a IPSec, y de las opciones ofrecidas seleccionamos *descarga de fichero*

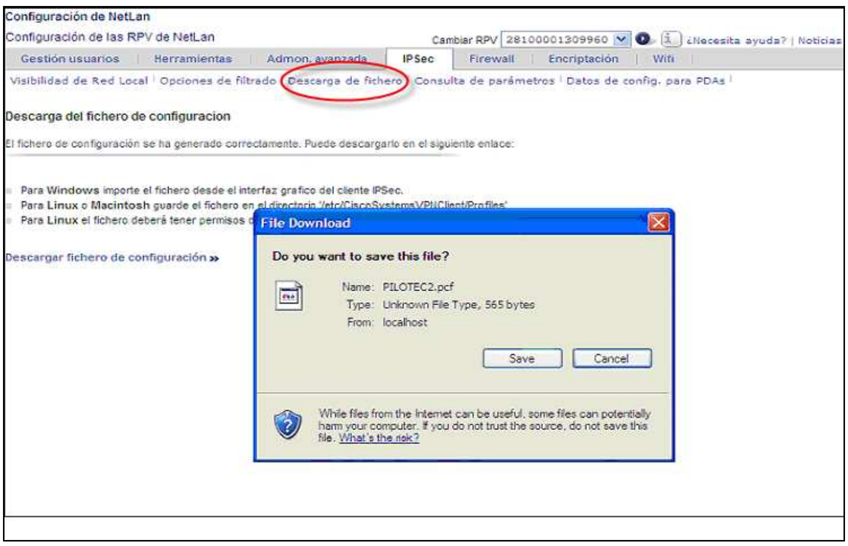


Figura 6: Descarga del fichero de configuración

Pulsaremos en el enlace '*Descarga fichero software IPSec*' y nos aparece un dialogo de descarga. **Importante**: el fichero se descargará con la extensión *.pcf de manera que es directamente importable al software IPSec.

Una vez descargado el software cliente IPSec y la correspondiente configuración, el administrador de la RPV-IP deberá distribuirlo a los usuarios de su RPV-IP que se conecten mediante este método.

3. INSTALACION Y CONFIGURACIÓN DEL ACCESO IPSEC POR PARTE DEL USUARIO

El usuario debe de instalarse el software IPSec en su ordenador, así como disponer del fichero de configuración correspondiente a su RPV-IP.

3.1 Cliente IPSec 5.0.07.0290 para Windows 7 / Windows Vista / Windows XP

3.1.1 Requisitos

El software Cisco VPN Client 5.0.07.0290 soporta las siguientes versiones de sistema operativo de cliente:

- Microsoft Windows 7 para sistemas de 32 bits y 64 bits con sus variantes: Starter, Home Premium, Professional). Se recomiendan instalaciones limpias, no actualizaciones desde Windows Vista o XP.
- Microsoft Windows Vista para sistemas de 32 bits y 64 bits (para evitar problemas se recomienda instalar SP2 o posteriores).
- Microsoft Windows XP
- Permite la compression LZS en sistemas de 64 bits
- Permite modems externos 3G que comercializa Movistar.
- Permite PC's Windows7 con módulos WWAN integrados.

  Para que funcione el cliente IPSec con estos dispositivos es posible que requiera actualizar el PC sobre todo si se ha instalado Windows 7 desde un Windows anterior (XP, Vista). Para instalar dicha actualización, es necesario que no haya instalado ninguna versión del cliente VPN cisco. Si ya está instalado se deberá desinstalar previamente y volver a instalar una vez actualizado.

  Para la realizar la actualización hay que ir a:

http://support.microsoft.com/kb/977999

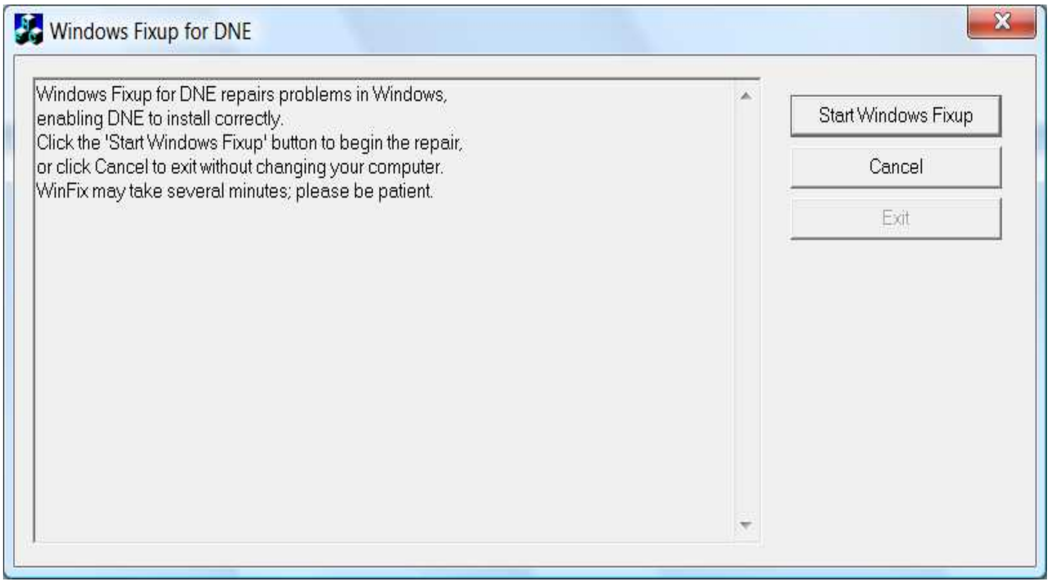
ó a la página de Citrix:

http://www.citrix.com/lang/English/lp/lp_1680845.asp

En esta página deberá descargar e instalar siguiendo todos los pasos que se indiquen:

ftp://ftpsupport.citrix.com/winfix.exe

Pulse botón"*Start Windows Fixup*" para comenzar la actualización:



A continuación descargue lo siguiente dependiendo de la versión de su sistema operativo:

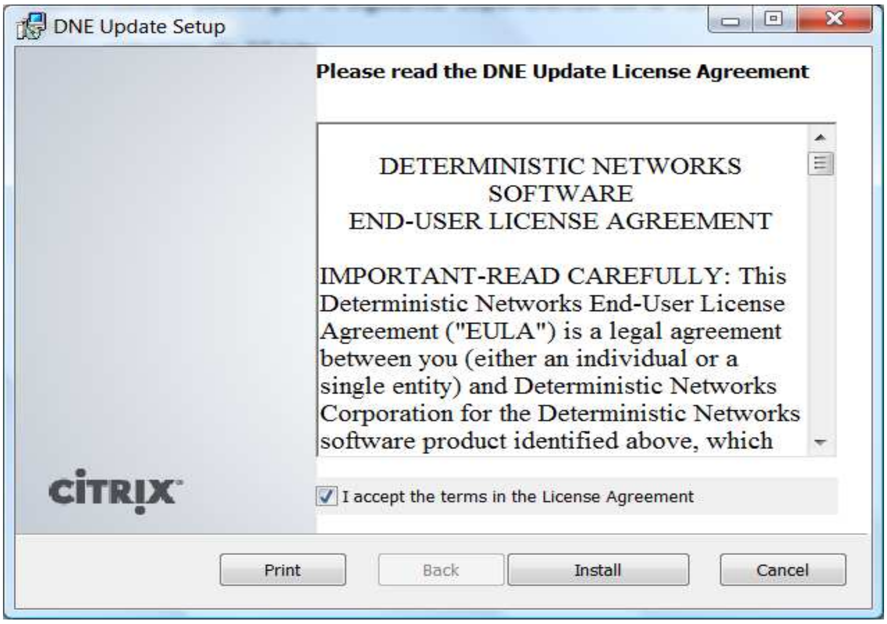
- sistemas de 32 bits:

  ftp://ftpsupport.citrix.com/dneupdate.msi

- sistemas de 64 bits:

  ftp://ftpsupport.citrix.com/dneupdate64.msi

Instalar siguiendo todos los pasos que indique:



El software Cisco VPN Client 5.0.07.0290 funciona sobre todos los sistemas operativos mencionados, y sobre múltiples tecnologías de acceso IP comercializadas por Movistar:

- Línea ADSL (GigADSL), tanto con configuración monopuesto como multipuesto.
- Línea ADSL (Alejandra) monopuesto y multipuesto.
- Sede Net-LAN con salida a Internet en red (PE/NAT).
- Sede Net-LAN WiFi.
- Línea ADSL Plus.
- Acceso Satélite bidireccional.
- Acceso conmutado RTC.
- Acceso Internet móvil por GPRS/UMTS MoviStar con módem externo 3G.

3.1.2 Restricciones

El software Cisco VPN Client 5.0.07.0290

- no está soportado sobre Tablet PC 2004/2005
- no está soportado en SO Windows 2000, NT, 98 y ME.
- no está soportado en combinación con Cisco Unified Video Advantage 2.1.2. ni con McAfee HIPS Patch 4 Build 688.

Los usuarios de Windows 7 deben tener cuidado con el uso de direcciones IP secundarias pues el cliente VPN utiliza la dirección IP primaria para el inicio de sesión. Sin embargo, el cliente utiliza la IP secundaria para transmitir todo el tráfico cuando la sesión está establecida. Esto puede generar situaciones imprevisibles en la conexión.

El software calificado resuelve limitaciones que existían en la versión 5.0.00:

- El cliente 5.0.00 está soportado sobre SO Windows Vista de 64 bits.

El software versión 5.0.07.0290 tiene detectado el siguiente reparo (a falta de realizar todas las pruebas):

- El cliente 5.0.07.0290 no es compatible con la funcionalidad SSO (Single Sign On) que gestiona las credenciales en las aplicaciones que solicitan usuario y password para autenticación. Este problema se ha detectado en los modelos de PC marca HP que tienen instalada la aplicación *HP Protect Tools Security Manager*.

La solución propuesta para este reparo es la desactivación de la funcionalidad SSO para la aplicación VPN Cisco. Para desactivar esta funcionalidad hay que seleccionar la conexión en la pantalla principal del cliente VPN Cisco y pulsar botón derecho.

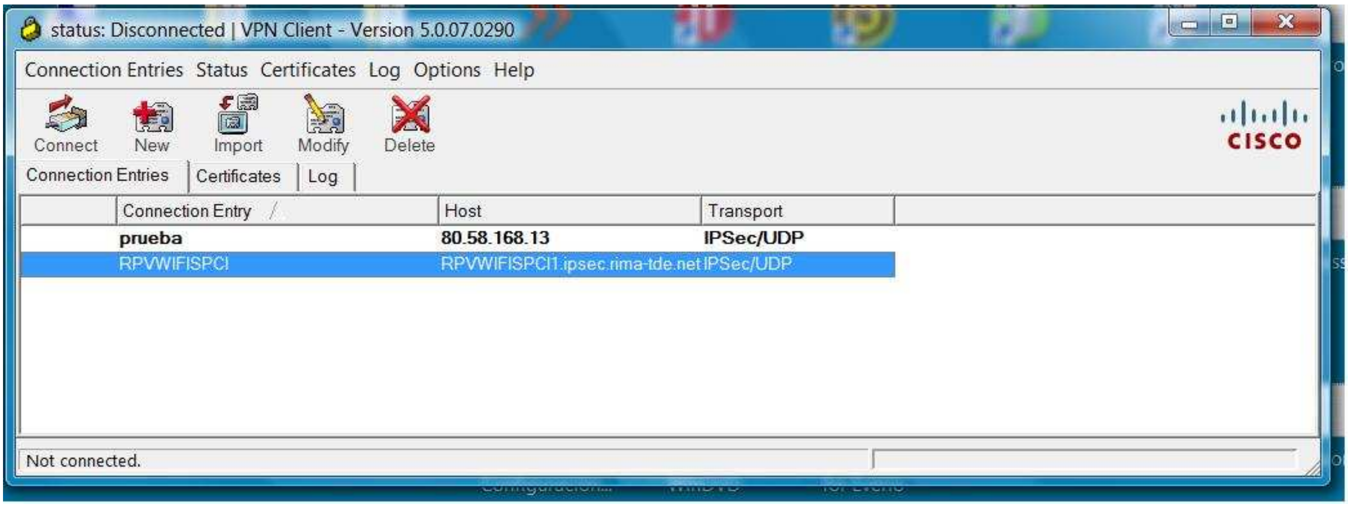


Figura 7: Página principal del cliente VPN Cisco

Se nos abrirá listado de acciones posibles con dicha conexión. Seleccionamos la opción "Modify" ó "Modificar" para que se nos muestren los datos de nuestra conexión:

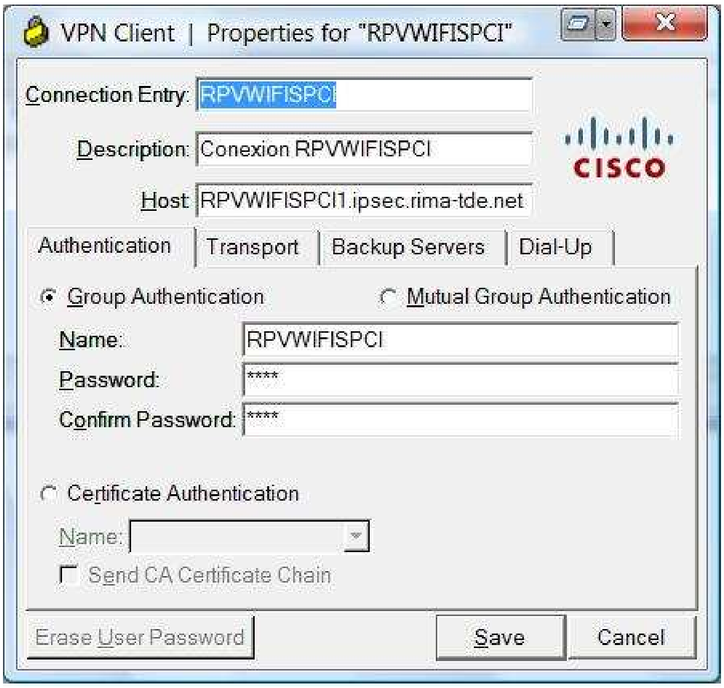


Figura 8: Perfil de la conexión

En la esquina superior derecha, junto al símbolo "X" que cierra la ventana aparece un icono con un símbolo de desplegable. Pinchamos en el símbolo del desplegable y nos muestra lo siguiente:



Figura 9: Detalle del desplegable en la ventana de conexión

Seleccionamos "No utilizar SSO con esta aplicación". De esta manera se desactivará la funcionalidad SSO para esta aplicación.

El software calificado <u>no resuelve limitaciones</u> que existían en la versión 5.0.00:

- La instalación de este software no se puede realizar sobre una versión actualizada de XP o Vista.

  Si se instala el cliente sobre una versión Windows7 actualizada de XP ó Vista se pueden producir problemas diversos: cliente no conecta, no se instala el adaptador,...

  Se deben utilizar instalaciones limpias de Windows 7.

- En indeterminados momentos de la ejecución del servicio, de repente, Windows Vista y 7 detecta e informa sobre un error de dirección IP duplicada detectada. Tras la aparición del mensaje no se pueden establecer conexiones IPSec.

  El reparo aún no está diagnosticado por Cisco y se ofrece una solución. Este reparo detectado implica que los clientes pueden tener problemas puntuales para establecer las conexiones, aunque estos problemas se resuelven con el siguiente **procedimiento**:

  Tras la aparición del mensaje no se pueden establecer conexiones IPSec y es necesario reiniciar el adaptador de red según el siguiente procedimiento:

  1. Abrir “Centro de Redes y recursos compartidos”
  2. Seleccionar “Cambiar configuración del adaptador”
  3. Habilitar el Virtual Adapter (“VA”—Cisco VPN Adapter)
  4. Con el botón derecho hacer clic en “Cisco VPN Adapter” y seleccionar "Diagnosticar” del menú contextual.
  5. Reiniciar el adaptador de red LAN “X”.

  Una vez reiniciado el adaptador el servicio vuelve a estar disponible.

3.1.3 Proceso de instalación

El software del cliente VPN Cisco v 5.07.0290 es diferente según el PC sea un sistema de 32 bits o de 64 bits. Habrá que verificar que sistema presenta el PC en el que se quiere instalar la aplicación. En cualquier caso, el proceso de instalación será el mismo.

Nada más ejecutar el fichero descargado, un cuadro de diálogo nos pide el directorio dónde queremos descomprimir el cliente IPSec. Se recomienda utilizar c:\temp\cisco pero se puede hacer en cualquier otro.

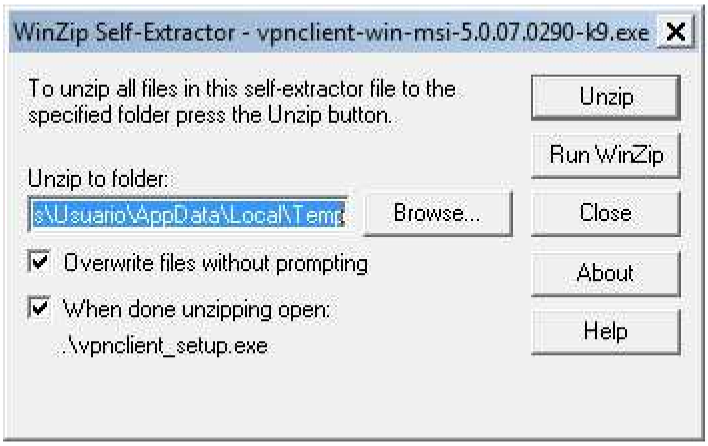


Figura 10: Directorio destino para la descompresión del fichero

Con la opción activada "*When done unzipping open: .\vpnclient_setup.exe*" en la figura anterior, una vez descomprimido se ejecuta automáticamente el fichero *vpnclient_setup.exe*, iniciando la instalación.

El software verificará si existe una versión anterior del software cliente IPSec, instalado previamente en el equipo, en caso de que así sea solicitará la desinstalación de la versión anterior y el posterior reinicio del equipo.

En primer lugar, nos aparecerá una ventana para seleccionar el idioma que se desee (inglés, francés o japonés); en la explicación que sigue se escogió el idioma inglés (English).

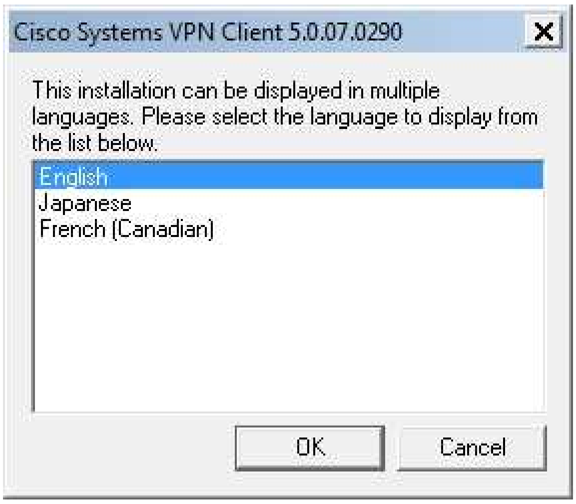


Figura 11: Selección de idioma

A continuación nos dará un mensaje de bienvenida, y pulsaremos '*next*' para continuar.

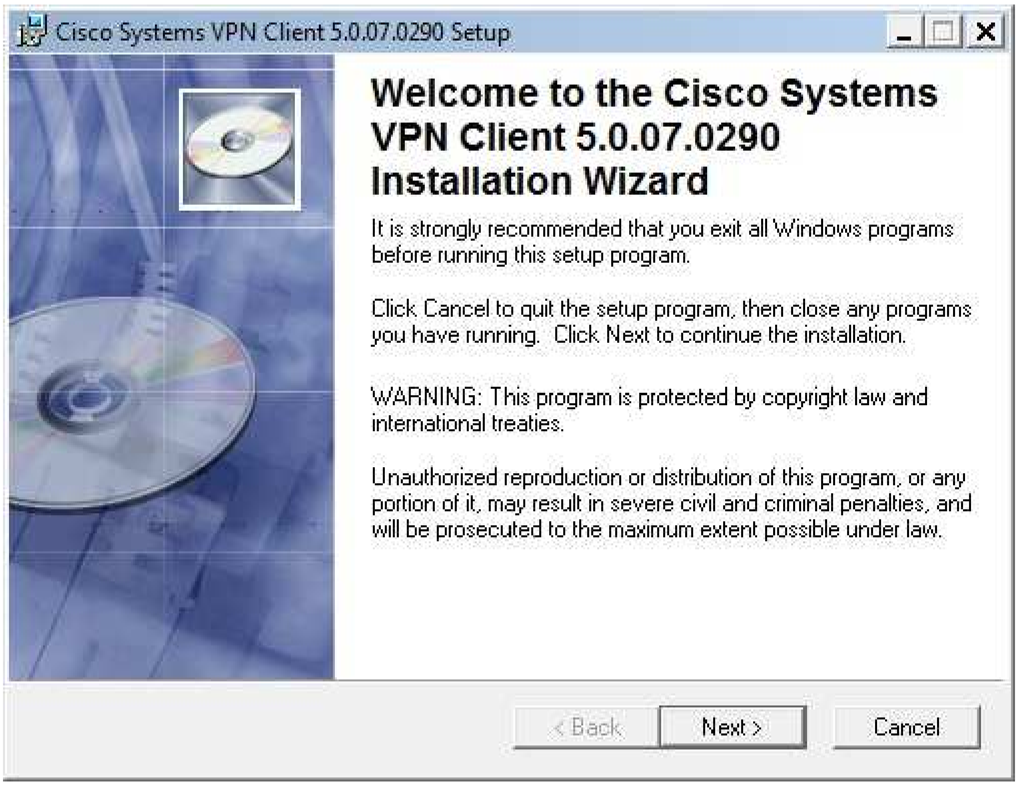


Figura 12. Pantalla de Bienvenida

Tras leer la licencia, se acepta pulsando '*I accept the license agreement*':

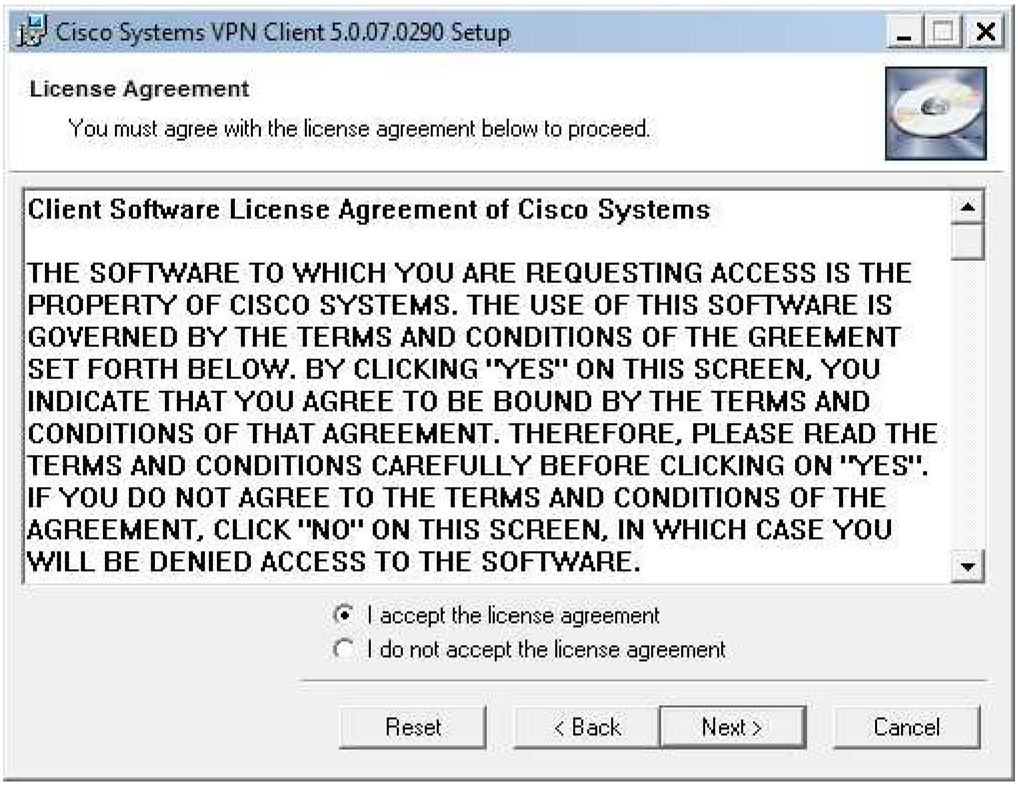


Figura 13: Licencia del software IPSec

En la siguiente acción se selecciona el directorio en el que se va instalar el software, por defecto se instalará en C:\Archivos de Programa\Cisco Systems\VPN Client, aunque se puede seleccionar otro directorio alternativo. A continuación se pulsa '*Next*' para continuar

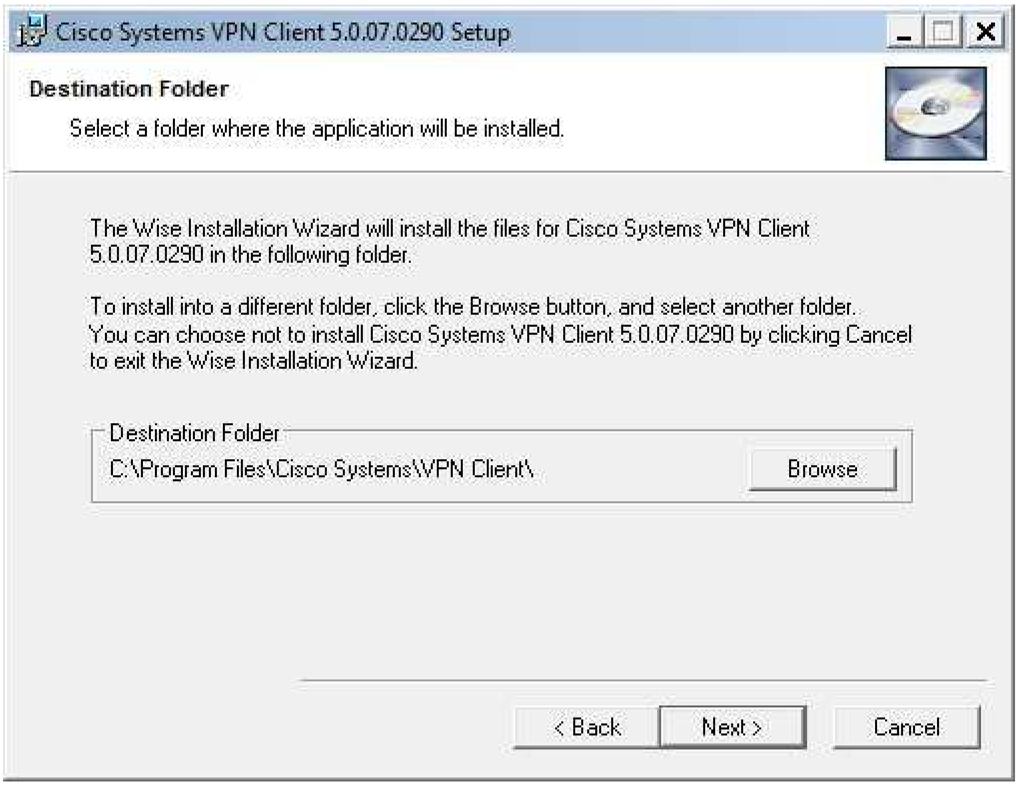


Figura 14: Selección del directorio de instalación

En este punto, el software te da la oportunidad de cambiar la información de la instalación, pulsamos “Next”:

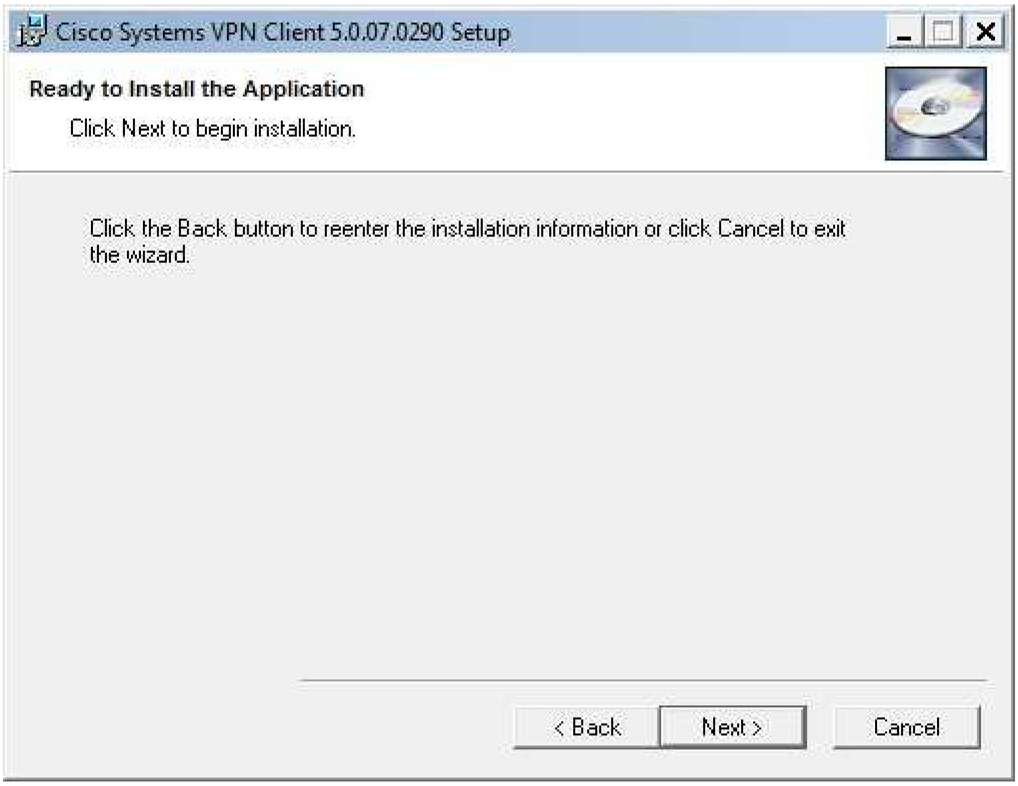


Figura 15: Confirmación de Instalación

A continuación, la aplicación actualiza el sistema copiando nuevos ficheros:

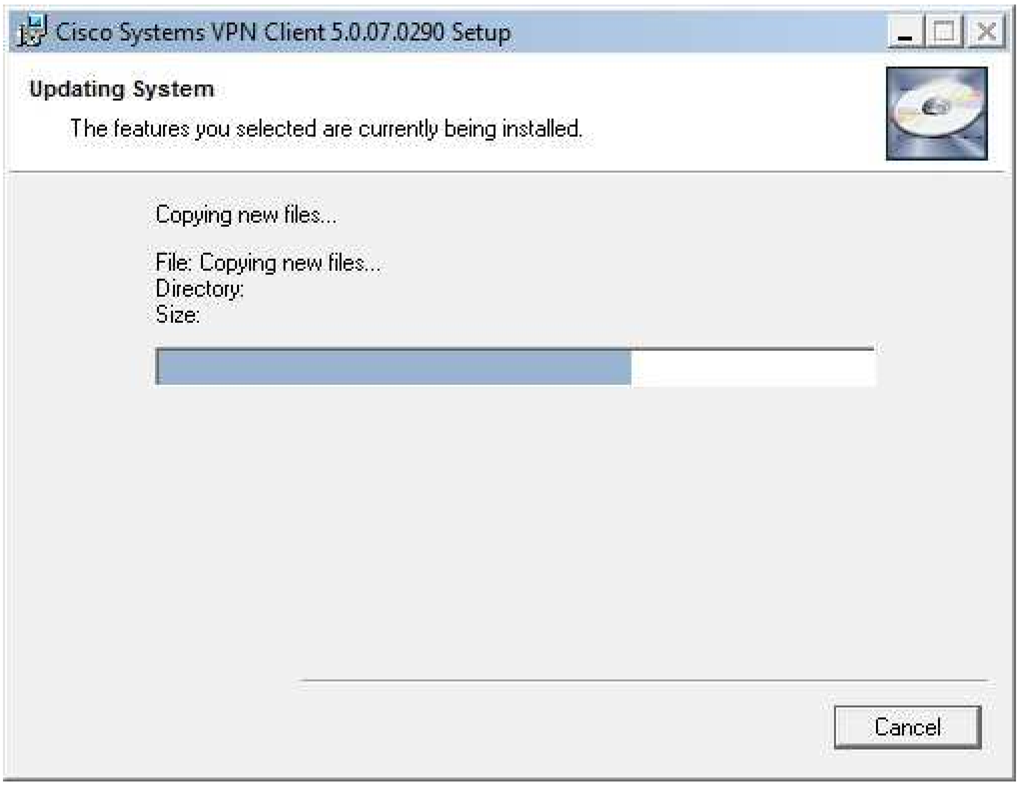


Figura 16: Copia de ficheros para actualizar sistema

Y comienza la instalación:

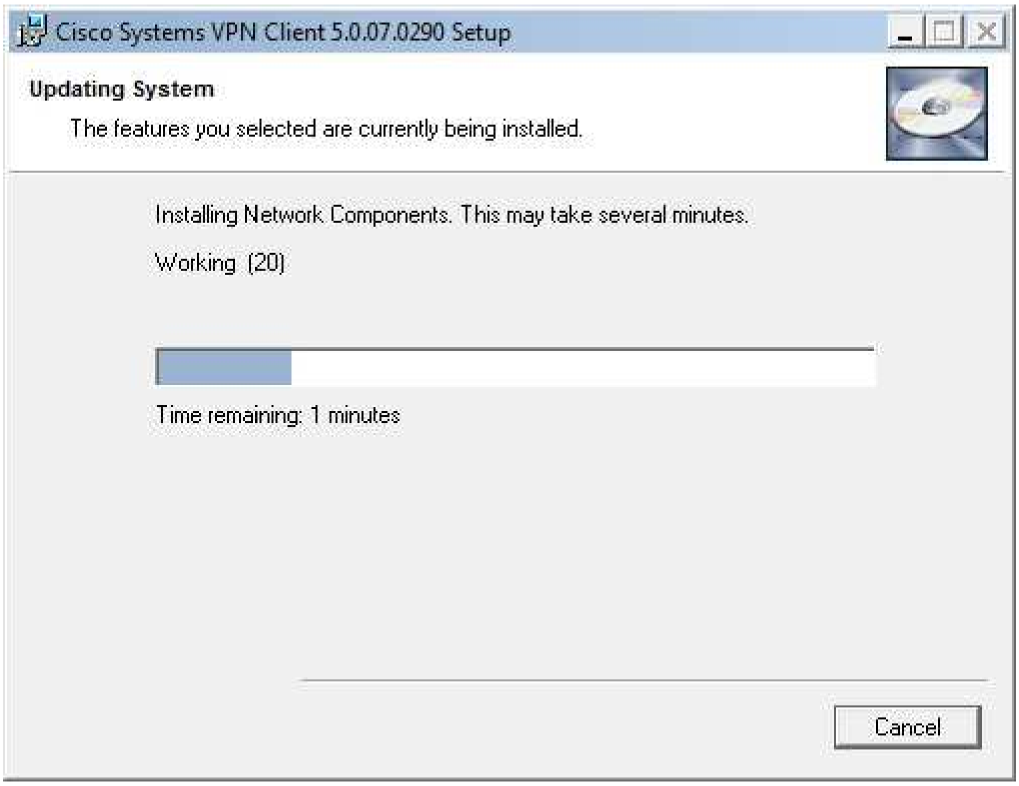


Figura 17: Instalación de Componentes de Red

Aparece la pantalla anunciando el final de la instalación y se pulsa '*Finish*'.

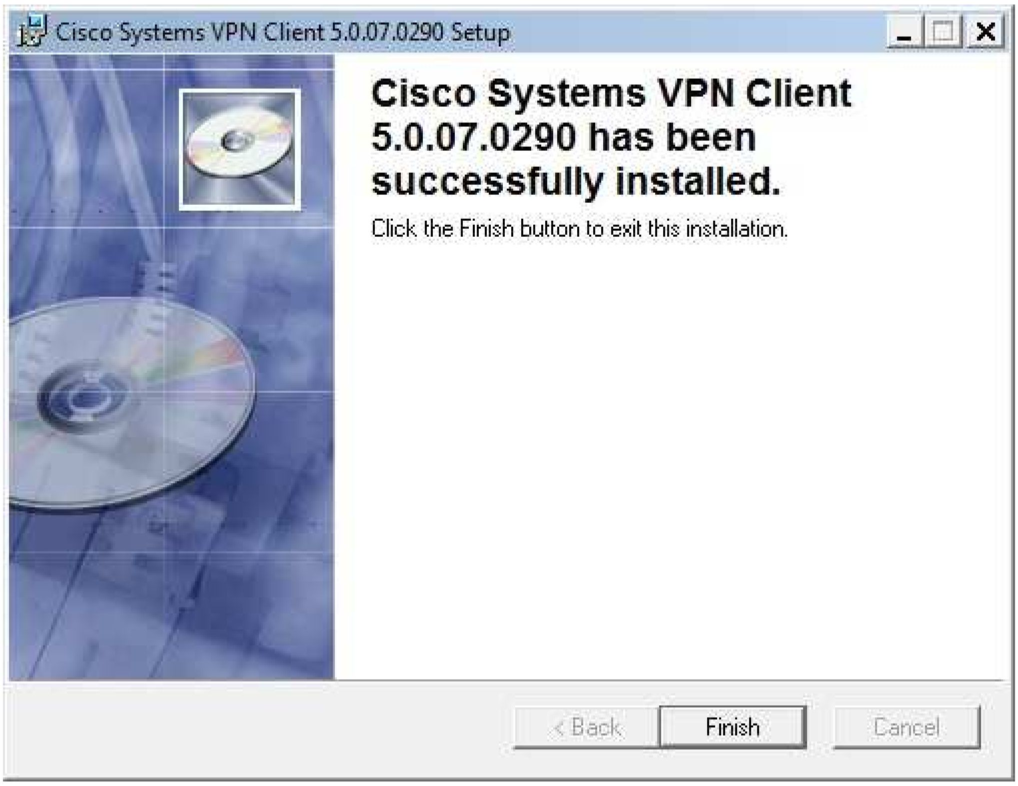


Figura 18: Fin del proceso de instalación

El ordenador debe reiniciarse para que la instalación se complete:

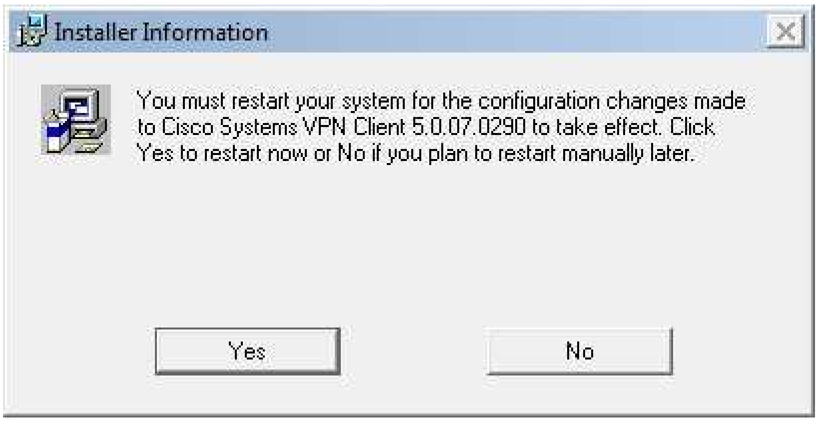


Figura 19: **Reinicio del sistema**

3.2 Cliente IPSec 5.0.00 para Windows Vista / XP/ 2003 Server / 2000

3.2.1 Requisitos

El software Cisco VPN Client 5.0.00 soporta las siguientes versiones de sistema operativo de cliente:

- Microsoft Windows Vista en sus variantes Home Basic, Home Premium, Business y Ultimate.
- Microsoft Windows XP.
- Microsoft Windows 2003 Server.
- Microsoft Windows 2000.

El software Cisco VPN Client 5.0.00 funciona sobre todos los sistemas operativos mencionados, y sobre múltiples tecnologías de acceso IP comercializadas por Movistar:

- Línea ADSL (GigADSL), tanto con configuración monopuesto como multipuesto.
- Línea ADSL (Alejandra) monopuesto y multipuesto.
- Sede Net-LAN con salida a Internet en red (PE/NAT).
- Sede Net-LAN WiFi.
- Línea ADSL Plus.
- Acceso Satélite bidireccional.
- Acceso conmutado RTC.
- Acceso Internet móvil por GPRS/UMTS Movistar.

3.2.2 Restricciones

El software calificado resuelve limitaciones que existían en la versión (4.6.03):

- Incompatibilidad del cliente Cisco VPN 4.6.03 con Panda Antivirus

- Fallo de resolución DNS con split tunneling en Windows XP.

El software V.5.0. tiene detectados los siguientes 3 reparos :

- La instalación de este software no se puede realizar sobre una versión actualizada de XP.

  Si se instala el cliente sobre una versión Vista actualizada de XP se pueden producir problemas diversos: cliente no conecta, no se instala el adaptador,...

  Se deben utilizar instalaciones limpias de Windows Vista.

- El cliente 5.0.00 no está soportado sobre SO Windows Vista de 64 bits.

- En indeterminados momentos de la ejecución del servicio, de repente, Windows Vista detecta e informa sobre un error de dirección IP duplicada detectada. Tras la aparición del mensaje no se pueden establecer conexiones IPSec.

  El reparo aún no está diagnosticado por Cisco, pudiendo ser un comportamiento derivado de algún mal funcionamiento propio de Windows Vista. Por el momento no esta confirmada la fecha objetivo prevista para una nueva versión que resuelva el reparo.

Este reparo detectado implica que los clientes pueden tener problemas puntuales para establecer las conexiones, aunque estos problemas se resuelven con el siguiente **procedimiento**:

Tras la aparición del mensaje no se pueden establecer conexiones IPSec y es necesario reiniciar el adaptador de red según el siguiente procedimiento:

6. Abrir "Redes y Centro de Seguridad"
7. Seleccionar "Gestión de Conexiones de Redes"
8. Habilitar el Virtual Adapter ("VA"—Cisco VPN Adapter)
9. Con el botón derecho hacer clic en "Cisco VPN Adapter" y seleccionar "Diagnóstico" del menú contextual.
10. Reiniciar el adaptador de red LAN "X".

Una vez reiniciado el adaptador el servicio vuelve a estar disponible.

3.2.3 Proceso de instalación

Nada más ejecutar el fichero descargado, un cuadro de diálogo nos avisa de una serie de limitaciones de esta versión del producto:



Figura 20: Mensaje de limitaciones del producto

Al pulsar aceptar nos pide el directorio dónde queremos descomprimir el cliente IPSec. Se recomienda utilizar c:\temp\cisco pero se puede hacer en cualquier otro.

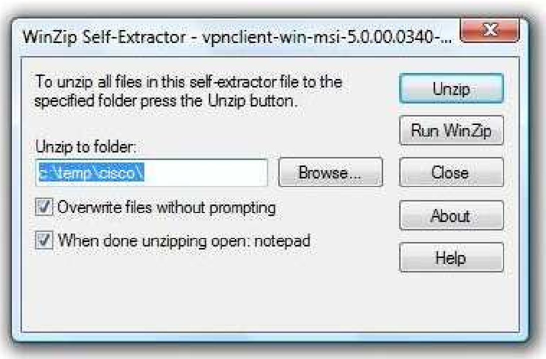


Figura 21: Directorio destino para la descompresión del fichero

Una vez descomprimido se accede al directorio dónde se haya descomprimido y se ejecuta el fichero vpnclient_setup.

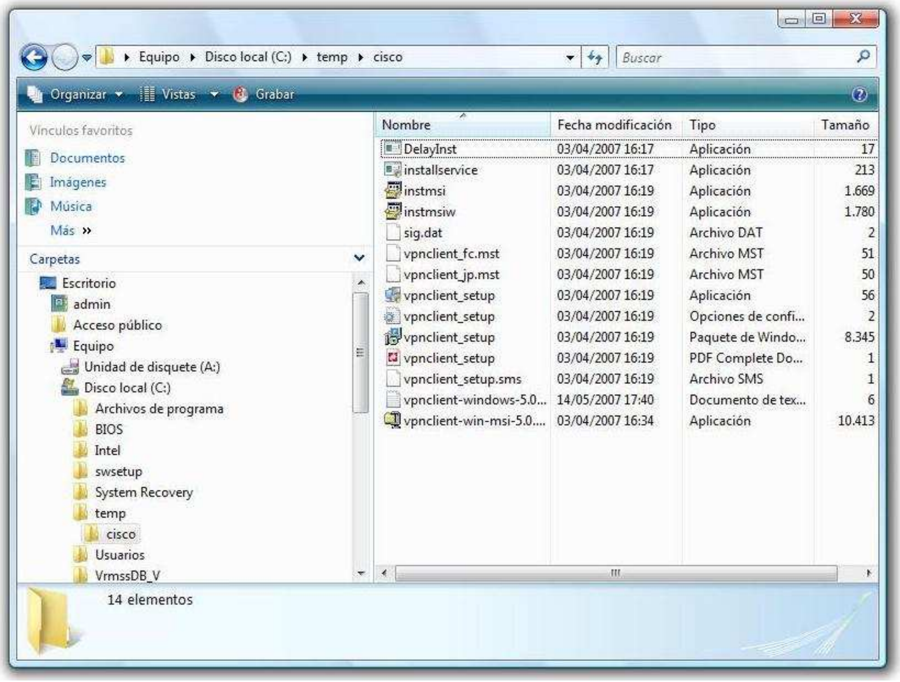


Figura 22: Ficheros descomprimidos

El software verificará si existe una versión anterior del software cliente IPSec, instalado previamente en el equipo, en caso de que así sea solicitará la desinstalación de la versión anterior y el posterior reinicio del equipo.

En primer lugar, nos aparecerá una ventana para seleccionar el idioma que se desee (inglés, francés o japonés); en la explicación que sigue se escogió el idioma inglés (English).



Figura 23: Selección de idioma

A continuación nos dará un mensaje de bienvenida, y pulsaremos '*next*' para continuar.

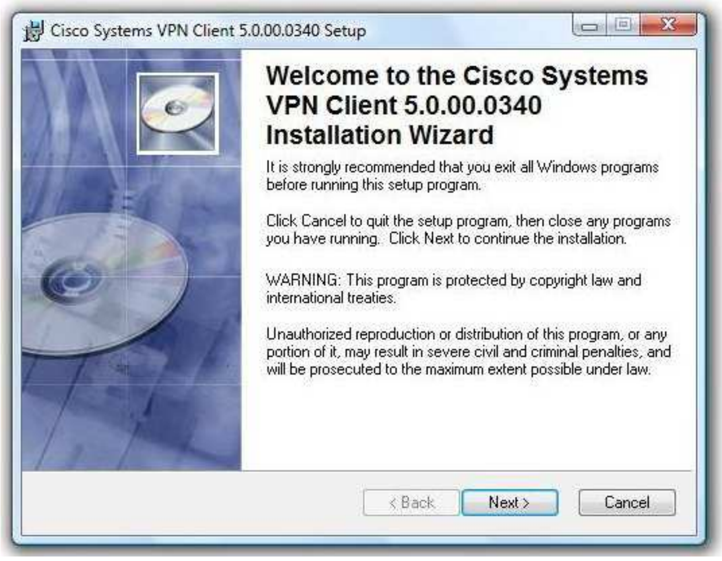


Figura 24. Pantalla de Bienvenida

Tras leer la licencia, se acepta pulsando '*yes*'



Figura 25: Licencia del software IPSec

En la siguiente acción se selecciona el directorio en el que se va instalar el software, por defecto se instalará en C:\Archivos de Programa\Cisco Systems\VPN Client, aunque se puede seleccionar otro directorio alternativo. A continuación se pulsa '*Next*' para continuar

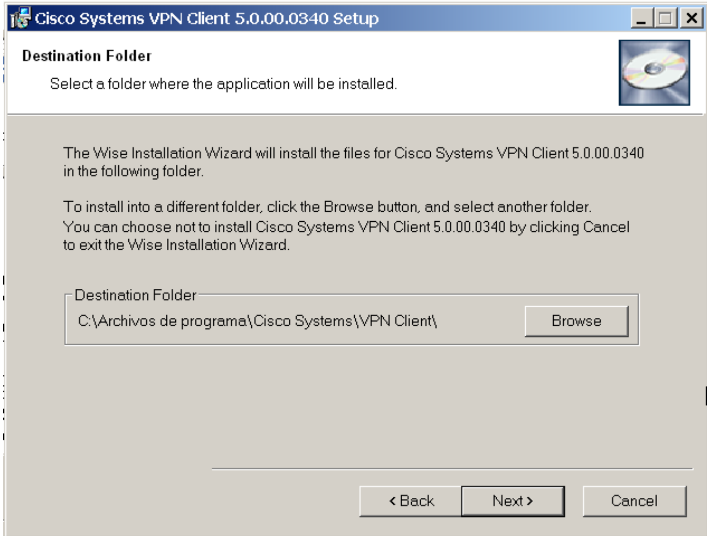


Figura 26: Selección del directorio de instalación

El software inicia la instalación en el equipo:

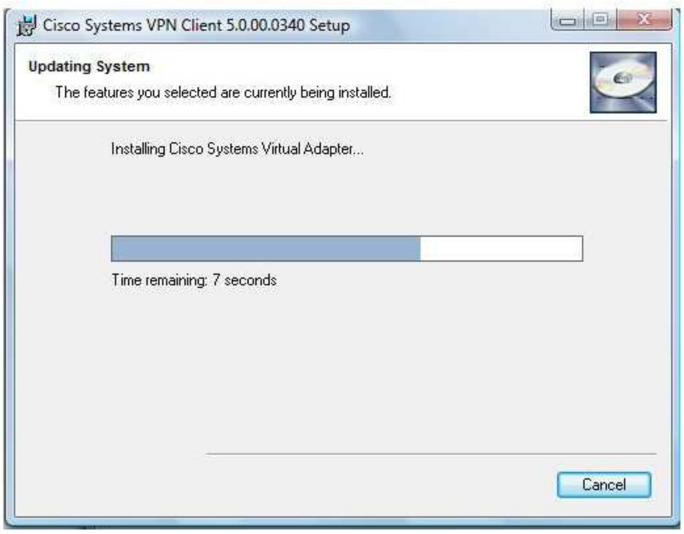


Figura 27: Instalación del software

Aparece la pantalla anunciando el final de la instalación y se pulsa '*Finish*'.



Figura 28: Fin del proceso de instalación

El ordenador debe reiniciarse para que la instalación se complete:

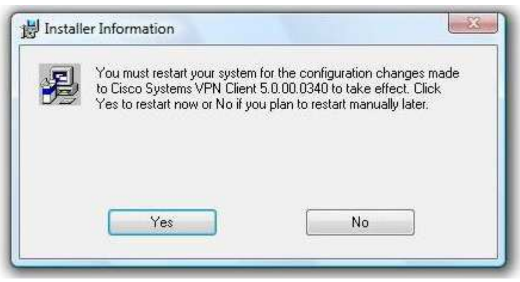


Figura 29: Reinicio del sistema

3.3 Cliente IPSec 4.6.03 para Windows NT / 98 / Me

3.3.1 Requisitos

El software Cisco VPN Client 4.6.03 soporta las siguientes versiones de sistema operativo de cliente:

- Microsoft Windows NT
- Microsoft Windows 98.

- Microsoft Windows ME.

3.3.2 Restricciones

El software posee las siguientes limitaciones:

- Incompatibilidad del cliente Cisco VPN 4.6.03 con Panda Antivirus

- Fallo de resolución DNS con split tunneling en Windows XP.

3.3.3 Proceso de instalación

Al ejecutar el fichero se descomprime y nos pide el directorio dónde queremos descomprimirlo. Se recomienda utilizar c:\temp pero se puede hacer en cualquier otro. Una vez descomprimido se accede al directorio dónde se haya descomprimido y se ejecuta el fichero vpnclient_setup.

El software verificará si existe una versión anterior del software cliente IPSec, instalado previamente en el equipo, en caso de que así sea solicitará la desinstalación de la versión anterior y el posterior reinicio del equipo.

En primer lugar, nos aparecerá una ventana para seleccionar el idioma que se desee (inglés, francés o japonés); en la explicación que sigue se escogió el idioma inglés (English).

A continuación nos dará un mensaje de bienvenida, y pulsaremos '*next*' para continuar.

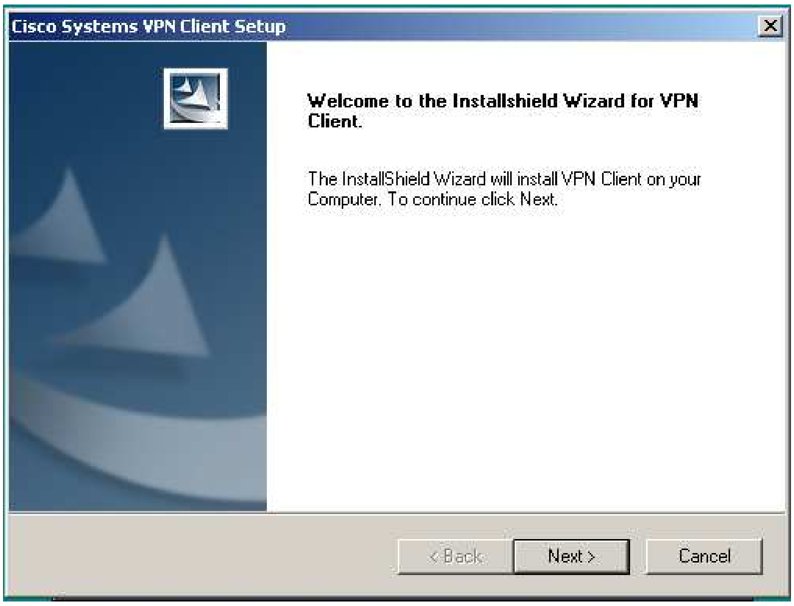


Figura 30. Pantalla de Bienvenida

Tras leer la licencia, se acepta pulsando '*yes*'

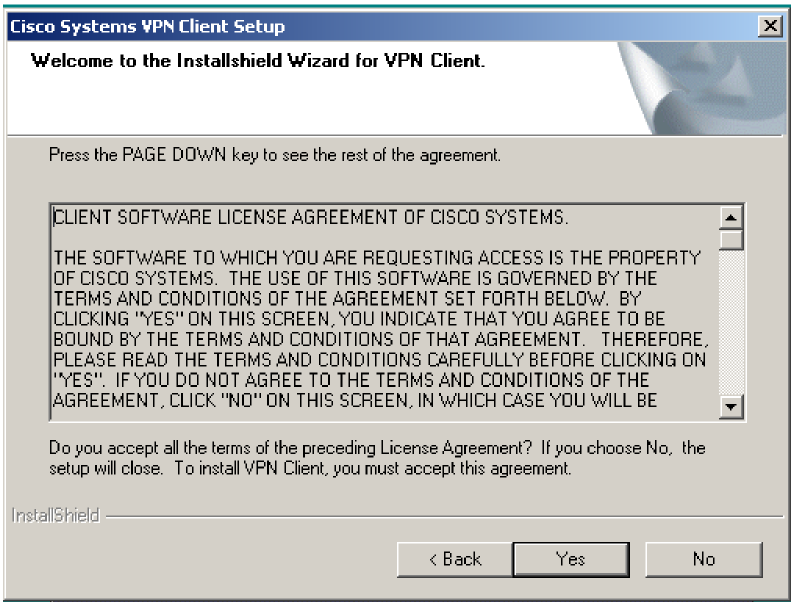


Figura 31: Licencia del software IPSec

En la siguiente acción se selecciona el directorio en el que se va instalar el software, por defecto se instalará en C:\Archivos de Programa\Cisco Systems\VPN Client, aunque se puede seleccionar otro directorio alternativo. A continuación se pulsa '*Next*' para continuar

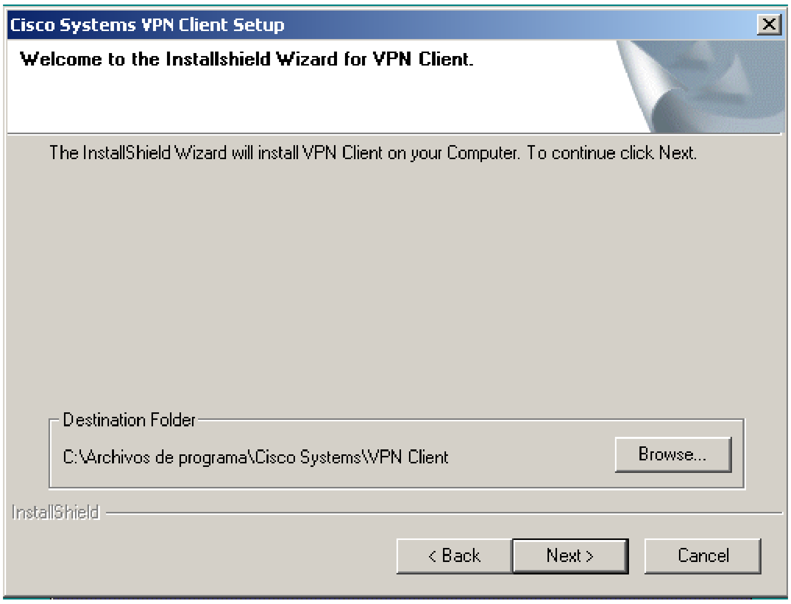


Figura 32: Selección del directorio de instalación

El software inicia la instalación en el equipo:

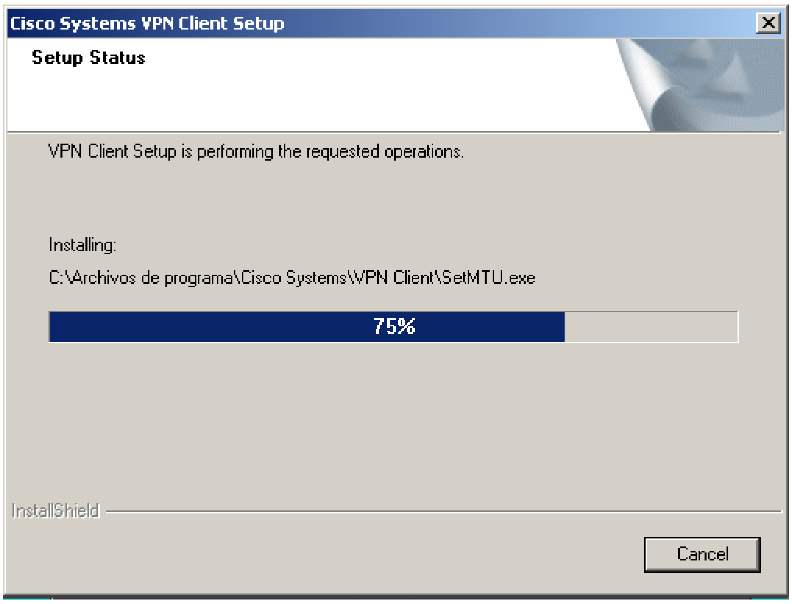


Figura 33: Instalación del software

Aparece la pantalla anunciando el final de la instalación y se pulsa '*Finish*'. El ordenador debe reiniciarse para que la instalación se complete:



Figura 34: Fin del proceso de instalación

3.4 Cliente IPSec en otros Sistemas Operativos

3.4.1 Sistema Operativo Linux

3.4.1.1 Requisitos

Antes de instalar el cliente IPSec en un sistema Linux se debe comprobar lo siguiente :

- Versión Linux compatible con las librerías glibc Version 2.1.1-6 o posterior y versión de Kernel 2.2.12 o posterior. En las pruebas se ha utilizado Linux Debian con version de kernel 2.4.27.
- El cliente no soporta kernel SMP (multiprocesador).
- En caso de que se tenga un firewall (i.e. ipchains o iptables) se debe desactivar o configurar para que el tráfico siguiente sea permitido:
    - UDP: puerto 500
    - UDP: puerto 10000
    - IP: protocolo 50 (ESP)
    - NAT-T: puerto 4500
- Se deben tener instaladas en el sistema las fuentes del kernel que se usaron para compilarlo.

3.4.1.2 Proceso de Instalación

Tras verificar todos los puntos anteriormente citados se debe obtener el fichero de instalación "*vpnclient-linux-4.6.00.0045-k9.tar.gz*". En primer lugar se descomprime con el comando siguiente:

```
tar –zxf <nombre fichero>
```

El fichero se descomprimirá en un directorio ../vpnclient/ por lo que se debe ir a dicho directorio y ejecutar la instalación:

```
cd vpnclient
./vpn_install
```

Durante la instalación se formulan las tres preguntas siguientes:

```
Directory where binaries will be installed [/usr/local/bin]

Automatically start the VPN service at boot time [yes]no

Directory containing linux kernel source code [/lib/modules/2.4.27/build]
```

Los valores que aparecen entre corchetes son los que el programa propone por defecto, en la segunda pregunta si se responde "*no*", se deberá iniciar el servicio manualmente cada vez que se quiera usar el cliente con el comando /etc/init.d/vpnclient_init start tal y como el programa indica al final de la instalación.

La última pregunta nos especifica la ubicación de las fuentes del kernel que el programa ha encontrado, si no estuvieran instaladas el valor que nos ofrecería el programa sería "*[]*" por lo que la instalación del cliente nos daría un error. Antes de volver a relanzar el programa se deben instalar las fuentes.

A continuación se muestra el proceso correcto de instalación en el PC del laboratorio de pruebas:

```
Multimedia:/tmp/vpnclient# ./vpn_install
Cisco Systems VPN Client Version 4.6.00 (0045) Linux Installer
Copyright (C) 1998-2004 Cisco Systems, Inc. All Rights Reserved.

By installing this product you agree that you have read the
```

license.txt file (The VPN Client license) and will comply with

its terms.

Directory where binaries will be installed [/usr/local/bin]

Automatically start the VPN service at boot time [yes]no

In order to build the VPN kernel module, you must have the

kernel headers for the version of the kernel you are running.

Directory containing linux kernel source code [/lib/modules/2.4.27/build]

* Binaries will be installed in "/usr/local/bin".
* Modules will be installed in "/lib/modules/2.4.27/CiscoVPN".
* The VPN service will *NOT* be started automatically at boot time.
* Kernel source from "/lib/modules/2.4.27/build" will be used to build the module.

Is the above correct [y]

Shutting down /opt/cisco-vpnclient/bin/vpnclient: module cisco_ipsec is not running.

Stopped: /etc/init.d/vpnclient_init (VPN init script)

Making module

Copying module to directory "/lib/modules/2.4.27/CiscoVPN".

Already have group 'bin'

Creating start/stop script "/etc/init.d/vpnclient_init".

  /etc/init.d/vpnclient_init

Installing license.txt (VPN Client license) in "/opt/cisco-vpnclient/":

Installing bundled user profiles in "/etc/opt/cisco-vpnclient/Profiles/":

* Replaced Profiles: sample

```
Copying binaries to directory "/opt/cisco-vpnclient/bin".
Adding symlinks to "/usr/local/bin".
  /opt/cisco-vpnclient/bin/vpnclient
  /opt/cisco-vpnclient/bin/cisco_cert_mgr
  /opt/cisco-vpnclient/bin/ipseclog
Copying setuid binaries to directory "/opt/cisco-vpnclient/bin".
  /opt/cisco-vpnclient/bin/cvpnd
Copying libraries to directory "/opt/cisco-vpnclient/lib".
  /opt/cisco-vpnclient/lib/libvpnapi.so
Copying header files to directory "/opt/cisco-vpnclient/include".
  /opt/cisco-vpnclient/include/vpnapi.h

Setting permissions.
  /opt/cisco-vpnclient/bin/cvpnd (setuid root)
  /opt/cisco-vpnclient (group bin readable)
  /etc/opt/cisco-vpnclient (permissions not changed)
* You may wish to change these permissions to restrict access to root.
* You must run "/etc/init.d/vpnclient_init start" before using the client.
* You will need to run this script every time you reboot your computer.
```

Cada vez que se reinicia el PC se debe iniciar el servicio del cliente IPSEC con el comando:

```
/etc/init.d/vpn_client start
```

Este comando permite diversas opciones, i.e. parar el servicio, ver el estado del servicio, etc:

/etc/init.d/vpn_client {start|stop|restart|reload|status}

3.4.2 Sistema Operativo Mac OS X

3.4.2.1 Requisitos

El cliente IPSEC (versión *4.6.00.0045)* para Mac OS X funciona para cualquier *Power Macintosh* o máquinas compatibles con versiones de sistema operativo 10.2 o posteriores y 30 MB de espacio en el disco duro.

El cliente IPSEC (versión 4.9.01.0280) para MAC OS es compatible con versiones de sistema operativo 10.4, 10.5 y 10.6 y se requiere al menos 50 MB de espacio en el disco duro. Esta versión no es compatible con sistemas de 64 bits.

3.4.2.2 Proceso de Instalación

El cliente IPSEC se instala mediante doble clic en el ejecutable para Macintosh: "*vpnclient-darwin-4.6.00.0045-GUI-k9.dmg*" *ó "vpnclient-darwin-4.9.01.0280-universal-k9.dmg*", *según el Sistema Operativo.* El cliente tiene un interfaz gráfico idéntico al de Windows por lo que se deben seguir los pasos indicados en el ejecutable.

3.5 Configuración del cliente IPSec

Previamente se debe haber instalado el cliente IPSec y haber disponer del fichero de configuración que nos habrá facilitado el Administrador de nuestra RPV-IP.

La configuración del cliente IPSec es similar en todos los sistemas operativos.

3.5.1 Configuración en el S.O. Windows

1. Arranque el cliente IPSec: Vamos a la barra de inicio del sistema operativo y ejecutamos el programa VPN Client.



Figura 35: Ejecución del cliente IPSec

2. Aparecerá la pantalla: principal del programa, que podemos ver en la figura siguiente

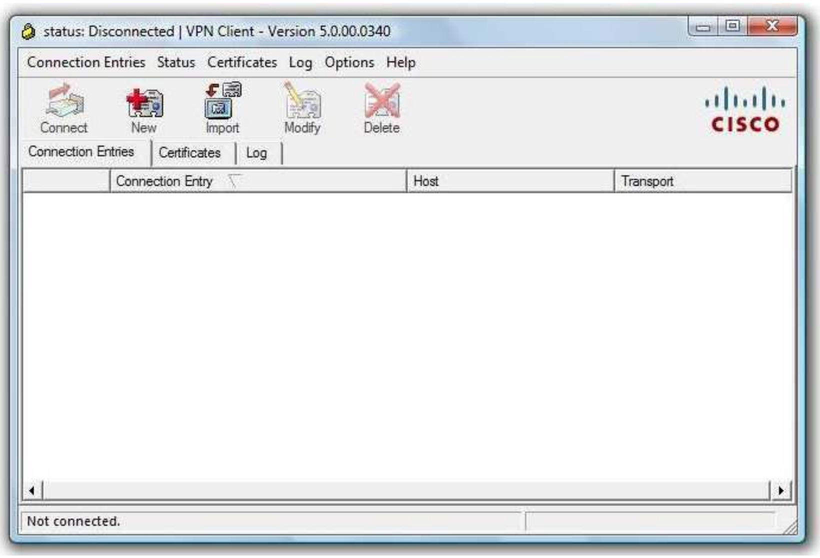


Figura 36: Pantalla principal del cliente IPSec

3. Pulse en el menú Import para crear la conexión.

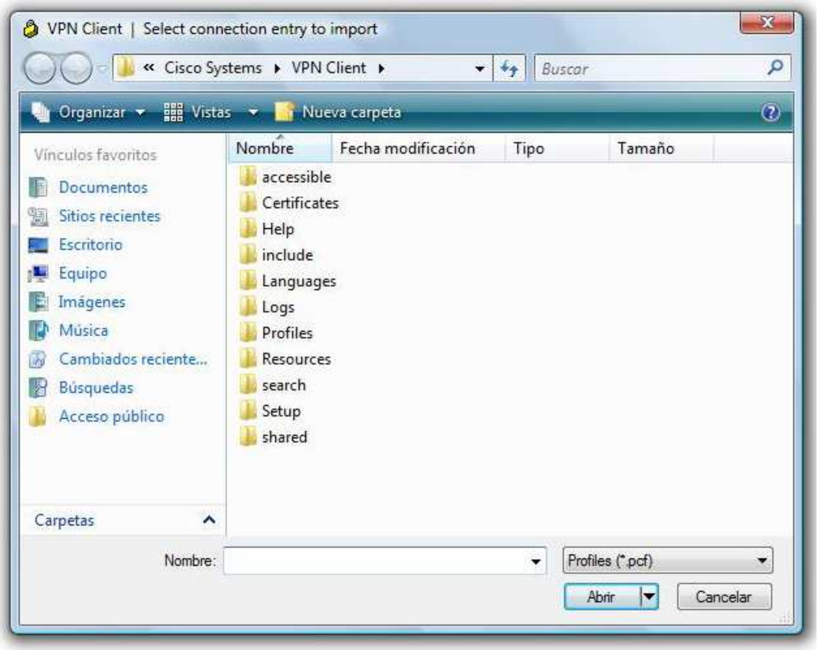


Figura 37: Creando la conexión por IPSec (paso 1)

Navegaremos hasta encontrar el fichero de configuración de la RPV-IP que habremos descargado o recibido previamente:

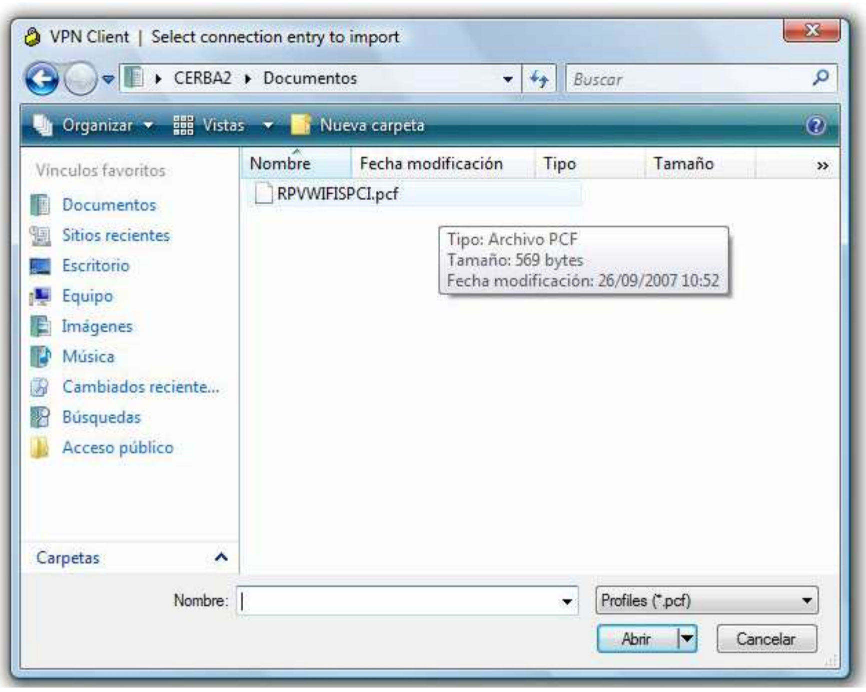


Figura 38: Creando la conexión por IPSec (paso 2)

Seleccionando el archivo pcf pulsaremos el botón'*Abrir*' y realizaremos la importación:



Figura 39: Creando la conexión por IPSec (paso 3)

4. Una vez importado, en la pantalla principal del programa nos aparecerá la conexión importada y pulsaremos '*Connect*' para establecer la conexión con nuestra RPV-IP. Durante el establecimiento de conexión, se le pedirá un nombre y una clave (que serán los asignados previamente por el administrador de nuestra RPV-IP) para autenticarse.



Figura 40: Usuario y contraseña para la conexión

Se debe teclear en Username el nombreusuario@nemónicodeRPV que debemos conocer. Pulsando *OK* ya estamos conectados:

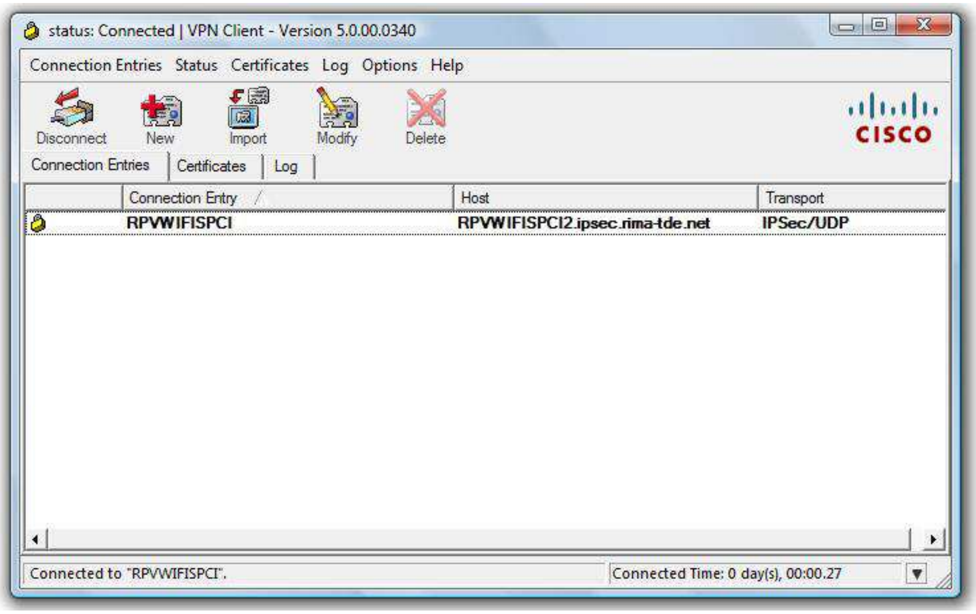


Figura 41: Pantalla inicial con la conexión iniciada

Aparece también un pequeño icono en la barra de tareas (un candado cerrado).

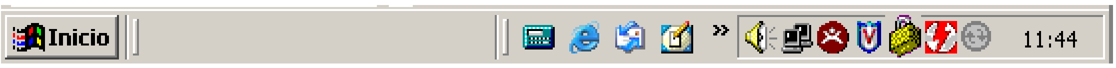


Figura 42: Icono de conexión establecida

3.5.2 Configuración manual

Es posible configurar el cliente IPSec, de forma manual, es decir introduciendo los parámetros correspondientes.

Los pasos a seguir son los siguientes:

1. Ejecutamos el cliente IPSec y seleccionamos '*New*' para crear una nueva conexión, nos aparece la pantalla siguiente:

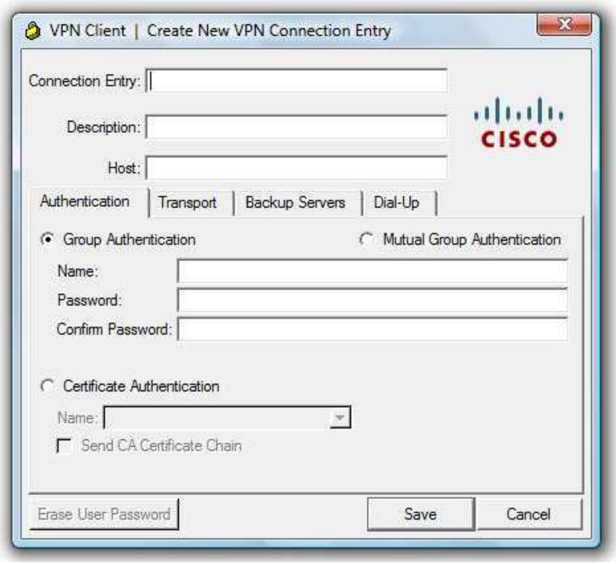


Figura 43: Configuración manual de la conexión

donde tendremos que rellenar cada uno de los campos siguientes:

- Connection Entry: Introducimos un nombre para identificar la nueva conexión.
- Description: descripción de la conexión
- Host: nombre del terminador de túneles contra el que se establecerá la conexión. Este dato aparece en los informes de configuración de los remotos IPSec. La forma del mismo es: Mnemónico_de_la_RPVIP1.ipsec.rima-tde.net, así si el mnemónico de nuestra RPV-IP es netlan, el nombre del Host será: netlan1.ipsec.rima-tde.net.

Seleccionamos la opción por defecto: 'Group Authentication' y rellenamos los campos siguientes:

- Name: tendremos que introducir el mnemónico de la RPV-IP.
- Password: el password será el mnemónico de la RPV-IP.
- Comfirm Password: volveremos a introducir el password para verificar que ha sido bien introducido.

Una vez que hemos rellanado todos los campos, pulsamos el botón '*Save*' para salvar la configuración de la conexión. Volveremos a la pantalla inicial del cliente IPSec y nos aparecerá la nueva conexión creada. Pulsaremos '*Connect*' para establecer la conexión con nuestra RPV-IP.

Durante el establecimiento de conexión, se le pedirá un nombre y una clave (que serán los asignados previamente por el administrador de nuestra RPV-IP) para autenticarse, como se ha descrito en el apartado anterior.

3.5.3 Configuración en otros Sistemas Operativos

3.5.3.1 Configuración para Linux

El cliente IPSEC para Linux no tiene interfaz gráfico por lo que los perfiles se deben configurar mediante la edición de los ficheros *.pcf con los parámetros correctos. Los ficheros de los perfiles se encuentran en /etc/CiscoSystemsVPNClient/Profiles/*.pcf. Se incluye un fichero de ejemplo con el perfil que se ha usado para las pruebas del laboratorio. En el apartado 3 se explica exhaustivamente la configuración de todos los parámetros de este fichero.

```
[main]
Description=
Host=80.58.168.73
AuthType=1
GroupName=EDCs_Se
GroupPwd=
enc_GroupPwd=DC904E0959B1476AF97460EAD20935F468FD76A1B0BB82F6818E1A69D7C4
44F3B16FF4DE4A0AA2C28642AF3C99F0F660
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPPhonebook=
ISPCommand=
Username=usuario1@EDCs_Se
SaveUserPassword=0
UserPassword=
enc_UserPassword=
NTDomain=
```

EnableBackup=0

BackupServer=

EnableMSLogon=1

MSLogonType=0

EnableNat=1

TunnelingMode=0

TcpTunnelingPort=10000

CertStore=0

CertName=

CertPath=

CertSubjectName=

CertSerialHash=00000000000000000000000000000000

SendCertChain=0

PeerTimeout=90

EnableLocalLAN=0

La conexión se realiza mediante el comando:

vpnclient connect <nombre_perfil>

```
# vpnclient connect EDCs_Se
Cisco Systems VPN Client Version 4.6.00 (0045)
Copyright (C) 1998-2004 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.27 #3 Wed Nov 3 13:32:16 CET 2004 i686
Config file directory: /etc/opt/cisco-vpnclient

Initializing the VPN connection.
Contacting the gateway at 80.58.168.73
User Authentication for EDCs_Se...
```

The server has requested the following information to complete the user authentication:

Username [usuario1@EDCs_Se]:

Password []:

Authenticating user.

Negotiating security policies.

Securing communication channel.

Your VPN connection is secure.

VPN tunnel information.

Client address: 10.227.0.16

Server address: 80.58.168.73

Encryption: 168-bit 3-DES

Authentication: HMAC-SHA

IP Compression: None

NAT passthrough is active on port UDP 4500

Local LAN Access is disabled

El comando vpnclient permite otras opciones, las cuales se citan a continuación:

vpnclient connect <profile> [user <username>] [eraseusrpwd | pwd <password>] [nocertpwd]

vpnclient disconnect

vpnclient stat [reset][traffic] [tunnel] [route] [repeat]

vpnclient notify

vpnclient verify [autoinitconfig]

vpnclient autoinit

3.5.3.2 Configuración para Macintosh

La configuración del cliente IPSEC mediante interfaz gráfico es exactamente igual que para el cliente IPSEC de windows, ver apartado 2.1.2 y 3 del presente documento. Los ficheros de los perfiles se encuentran en /etc/CiscoSystemsVPNClient/Profiles/*.pcf.

4. NUEVAS FUNCIONALIDADES

4.1 Activación de cortafuegos

En el acceso remoto IPSec (acceso remoto por Internet a su RPV-IP), el usuario puede simultanear la navegación Internet y la navegación Intranet a su RPV-IP gracias a que el "software" cliente en el PC dirige hacia su RPV-IP los paquetes IP cuyas direcciones destino son de la RPV, por medio de un túnel IPSec; el resto de paquetes se encaminan de la forma habitual por Internet (ya que un acceso IPSec se construye sobre una conexión a Internet ya existente).

El uso de "split tunneling" (así se llama esta capacidad) implica algunos problemas de seguridad: alguien puede entrar en el PC del usuario desde Internet y desde ese PC entrar en la RPV.

El cliente IPSec incluye un cortafuegos que proporciona seguridad cuando la opción de Split tunneling está habilitada y protege a la RPV-IP de ataques desde Internet mientras el usuario remoto está conectado a su red.

Este cortafuegos integrado es válido para:

- Cliente IPSec 5.0.00 sólo en Sistemas Operativos Windows 2000, 2003 y XP. No se aplica a los Sistemas Operativos Windows Vista.
- Cliente IPSec 4.6.03 para los Sistemas Operativos Windows NT / 98 / Me

.

Este cortafuegos integrado en el cliente IPSec configura las siguientes reglas de filtrado:

1. Todo lo que es cifrado es pasado al túnel para destino su RPV-IP.
2. Permite que pase todo el tráfico originado en el PC.
3. Todo lo que no es originado en el PC, es decir, que viene del exterior, es denegado.

Las reglas no son modificables, luego se aplicarán una vez que esté habilitada esta opción en el cliente IPSec.

Para habilitar el cortafuegos, seleccionamos el menú Options del cliente IPSec, la opción de Stateful Firewall (Always On)

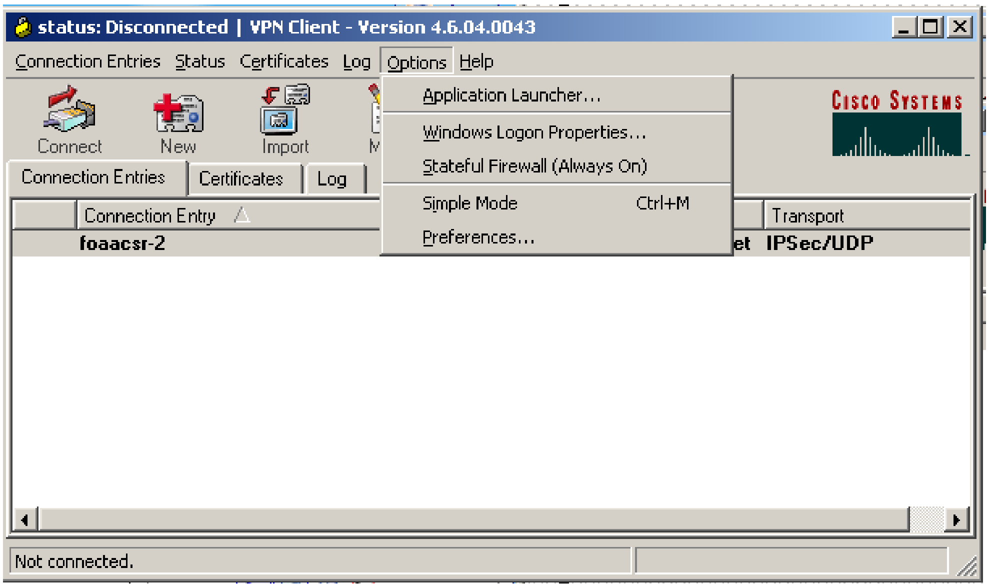


Figura 44 : Habilitación del Firewall

Cuando el cortafuegos está activado se verá un check en la opción correspondiente. Esta opción está deshabilitada por defecto y es conveniente habilitarla si la RPV tiene activa la opción de 'Split tunneling"

4.2 Cliente transparente a NAT

Esta funcionalidad permite utilizar el cliente IPSec cuando la conexión se realiza sobre una línea ADSL con un router configurado en la opción de multipuesto.

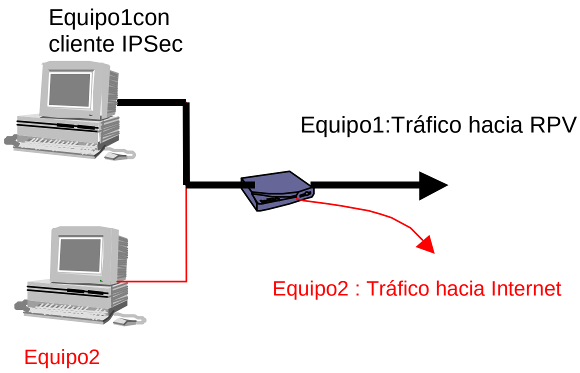


Figura 45: **ADSL multipuesto. Un usuario remoto**

Esta opción aparecerá marcada por defecto, no obstante es posible deshabilitarla. Para llegar a ella, marcamos la conexión y pulsamos sobre el icono titulado “Modify”:

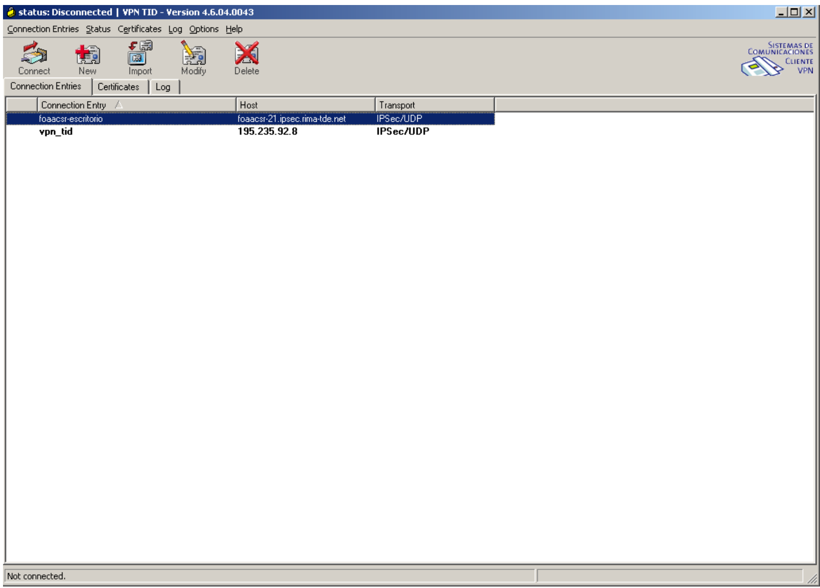


Figura 46: Cambiando las propiedades de una conexión

En la pestaña Transport, aparecerá la opción Enable Transparent Tunneling.

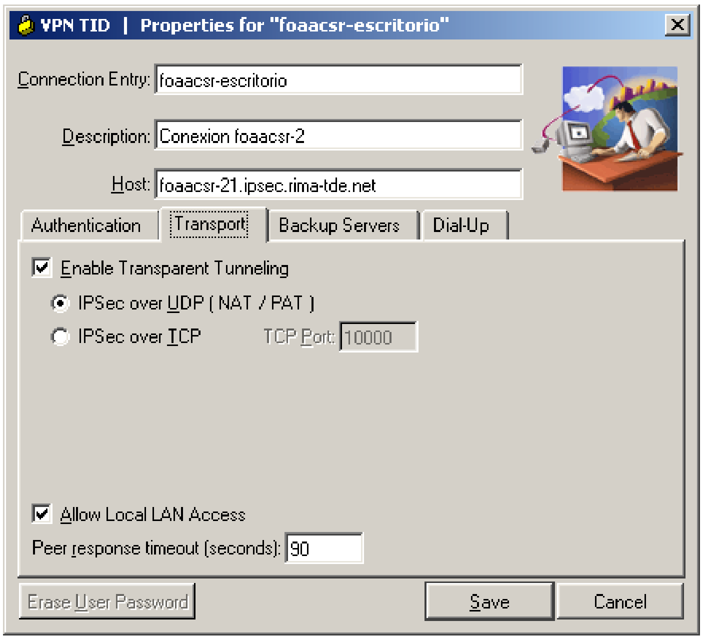


Figura 47: cliente IPSec transparente a NAT

Es posible mantener una sesión IPSec en el router, algunos equipos no soportan mantener más de una sesión IPSec simultánea, consulte la documentación del fabricante para saber si su equipo lo permite.